

Форма № ДН-7.02.1

Державний вищий навчальний заклад
«Донецький національний технічний університет»
Кафедра Прикладної математики та інформатики



«ЗАТВЕРДЖУЮ»

Перший проректор

Леонід Бачурін

2021 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ВБ 1.1 Інформаційна безпека

(шифр і назва навчальної дисципліни)

Рівень освіти: другий (магістерський)

Спеціальність (ості) 121 Інженерія програмного забезпечення
(шифр і назва спеціальності (тей))

Освітня програма Інженерія програмного забезпечення
(назва освітньої програми, для обов'язкових дисциплін)

Мова навчання: українська

Покровськ – 2021

Робоча програма навчальної дисципліни «**Інформаційна безпека**»
для здобувачів вищої освіти за спеціальністю 121 Інженерія програмного забезпечення
«18» січня 2021 року. – 8 с.

Розробник:

Маслова Н.О., к.т.н., доц., доц. каф. ПМІ

Робоча програма затверджена на засіданні кафедри прикладної математики і інформатики

(назва кафедри)

Протокол № 1 від «18» січня 2021 р.

Завідувач кафедрою

ПМІ

(підпис)

(Дмитрієва О.А.)
(прізвище та ініціали)

«18» січня 2021 р.

Схвалено науково-методичною комісією з галузі знань 12 Інформаційні технології
(шифр, назва)

Протокол № 1 від «19» січня 2021 р.

«19» січня 2021 р. Голова

(підпис)

(Башков Є.О.)
(прізвище та ініціали)

1. Загальна інформація

Форма навчання	Денна	Заочна
Статус	вибіркова дисципліна	
Обсяг в кредитах ЕКТС	7	
Обсяг в годинах за навчальним планом, разом:	210	
в тому числі:		
лекцій:	32	
практичні заняття:	XX	
лабораторні заняття:	48	
семінари:	XX	
самостійна робота:	130	
у т.ч. Курсова робота		
Форма підсумкового контролю	Екзамен	
Дисципліну викладають	Викладач 1: доц., к.т.н., доц.каф.ПМІ Маслова Н.О., https://donntu.edu.ua/knt/pmi_natalia.maslova@donntu.edu.ua Викладач 2: ст.викладач каф.ПМІ Ярош І.В., https://donntu.edu.ua/knt/pmi_iryana.yarosh@donntu.edu.ua	

Передумови для вивчення дисципліни: перелік дисциплін, які мають бути вивчені раніше: Основи інформаційної безпеки, Безпека програм та даних, Архітектура та проектування програмного забезпечення.

2. Мета вивчення навчальної дисципліни

Метою викладання дисципліни є оволодіння знаннями та вміннями, які утворюють теоретичний і практичний фундамент, необхідний для побудови систем захисту інформації й отримання навичок управління інформаційною безпекою.

Компетентності:

- ЗК1 – Здатність до абстрактного мислення, аналізу, синтезу
- ЗК3 – Здатність проведення теоретичних та прикладних досліджень на відповідному рівні
- ЗК5 – Здатність спілкуватися з представниками інших професійних груп різного рівня
- ЗК6 – Здатність удосконалювати свої навички на основі аналізу попереднього досвіду

ФК1 – Здатність аналізувати предметні області, формувати, аналізувати та моделювати вимоги до програмного забезпечення

ФК4 – Здатність розвивати і реалізовувати нові конкурентоспроможні ідеї в інженерії програмного забезпечення

ФК5 – Здатність оцінювати ступінь обґрунтованості застосування специфікацій, стандартів, правил і рекомендацій в професійній галузі та дотримуватися їх при реалізації процесів життєвого циклу програмного забезпечення

ФК6- Здатність ефективно керувати фінансовими, людськими, технічними та іншими проектними ресурсами

ФК9 – Здатність забезпечувати дотримання вимог щодо якості програмного забезпечення

Програмні результати навчання:

ПР1 – знати і системно застосовувати методи аналізу та моделювання прикладної області, виявлення інформаційних потреб і збору вихідних даних для проектування програмного забезпечення

ПР2 – Обґрунтовувати вибір методів формування вимог до програмної системи, розробляти, аналізувати та систематизувати вимоги

ПР6 – Аналізувати, оцінювати і вибирати методи, сучасні програмно-апаратні інструментальні та обчислювальні засоби, технології, алгоритмічні та програмні рішення для ефективного виконання конкретних виробничих задач з програмної інженерії

ПР8 – Проводити аналітичне дослідження параметрів функціонування програмних систем для їх валідації та верифікації, а також проводити аналіз обраних методів, засобів автоматизованого проектування та реалізації програмного забезпечення

ПР9 – знати і застосовувати сучасні професійні стандарти і інші нормативно-правові документи з інженерії програмного забезпечення

ПР10 – Вміти приймати організаційно-управлінські рішення в умовах невизначеності

ПР12 – Застосовувати моделі і методи оцінювання та забезпечення якості на всіх стадіях життєвого циклу програмного забезпечення

Вивчення дисципліни надає знання з основоположних принципів побудови та функціонування системи інформаційної безпеки (ІБ); архітектури побудови систем захисту інформації, функціональні можливості та управління модулями СЗІ.

3. Очікувані результати навчання

(для обов'язкових дисциплін)

Вміння орієнтуватися в різних архітектурних рішеннях побудови інформаційних систем захисту інформації; оформлювати прийняті рішення у вигляді комплексу технічної документації; проводити об'єктивний аналіз ефективності прийнятих технічних рішень; розробляти та будувати політику безпеки в організації та на підприємстві; проводити внутрішній аудит згідно розробленої політики безпеки.

4. Засоби діагностики результатів навчання

Засобами оцінювання та методами демонстрування результатів навчання можуть бути:

- екзамени;
- стандартизовані тести;
- індивідуальні та командні проекти;
- аналітичні звіти, реферати, есе;
- презентації результатів виконаних завдань та досліджень;
- виступи на наукових заходах.

5. Критерії оцінювання результатів навчання

Критерії оцінювання мають формулювати порядок оцінювання під час поточного контролю (за результатами практичних, лабораторних, семінарських занять та виконання індивідуальних або групових завдань) та підсумкового контролю.

Лр.1	Лр.2	Лр.3	Лр.4	Лр.5	Лр.6	Лр.7	Лр.8	Поточний контроль	Іспит	Максимальний бал
5	5	5	5	5	5	5	5	40	60	100

Примітка. Лр.1, Лр.2 і т.д. практичні роботи.

Сз1, Сз2 і т.д. семінарські заняття;

Лр1, Лр2 і т.д. лабораторні роботи.

В оцінку поточного контролю з виконання лабораторних робіт включено контрольні та поточні опитування.

Контроль виконання курсової роботи включає поточний контроль за виконанням розрахунків та захист перед комісією. Оцінка виконання та захисту курсової роботи проводиться за 100-бальною шкалою.

Приклад розподілу балів, які отримують студенти за виконання курсової роботи

Пояснювальна записка	Захист роботи	Сума
40	60	100

Схема оцінювання з урахуванням вимог Положення про організацію освітнього процесу. Результати підсумкового контролю оцінюються за 100-бальною шкалою та чотирибальною («відмінно», «добре», «задовільно», «незадовільно»).

Відповідність між шкалами встановлюється наступним чином:

Оцінка	
За 100-бальною шкалою	Для екзамену, курсового проекту(роботи), практики, диференційованого заліку, кваліфікаційного екзамену, випускної кваліфікаційної (дипломної) роботи (проекту)
90-100	відмінно
74-89	добре
60-73	задовільно
0-59	незадовільно

6. Програма навчальної дисципліни

6.1. Основні теми дисципліни

- Тема 1. Правові основи інформаційної безпеки.
- Тема 2. Стандарти інформаційної безпеки та менеджменту ІБ.
- Тема 3. Системи управління інформаційною безпекою. Вимоги.
- Тема 4. Поняття внутрішнього та зовнішнього аудиту ІБ
- Тема 5. Теорія ризиків, керування ризиками ІБ, ПЗ аналізу ризиків.
- Тема 6. Політики інформаційної безпеки.
- Тема 7 Організація інформаційної безпеки
- Тема 8. Керування активами та класифікація інформації
- Тема 9. Безпека, пов'язана з людськими ресурсами
- Тема 10. Фізична безпека та безпека середовища
- Тема 11. Управління взаємодією й експлуатацією
- Тема 12. Керування доступом
- Тема 13. Придбання, розробка і супровід інформаційних систем
- Тема 14. Управління інцидентами інформаційної безпеки
- Тема 15. Управління безперервністю діяльності (бізнесу)
- Тема 16. Відповідність законодавчим вимогам

6.2. Теми практичних (семінарських) занять

№ з/п	Назва теми	Кількість годин	
		Д.ф.н.	З.ф.н.
1	Проведення практичних занять не передбачено		
2			

...	Усього годин		
-----	--------------	--	--

6.3. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Лабораторна робота 1. Законодавча база менеджменту інформаційної безпеки	4
2	Лабораторна робота 2. Ідентифікація активів	4
3	Лабораторна робота 3. Аналіз погроз інформаційної безпеки, застосування інструментальних систем	6
4	Лабораторна робота 4. Керування ризиками ІБ, розробка контрзаходів	4
5	Лабораторна робота 5. Створення політик інформаційної безпеки	6
	Лабораторна робота 6. Менеджмент інформаційної безпеки	8
7	Лабораторна робота 7. Розробка програмних модулів захисту інформації	8
8	Лабораторна робота 8. Навички проведення внутрішнього аудиту	8
	Усього семестр	48
	Усього годин	48

6.4. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Тема 1. Нормативно-правове регулювання діяльності у галузі криптографічного захисту інформації.	8
2	Тема 2. Основні постулати першого стандарту інформаційної безпеки – «Помаранчевої книги»	8
3	Тема 3. Придбання навичок з роботи з системами захисту інформації та розрахунку ризиків. Метод CRAMM Види аналізу ризиків проєктів.	8
4	Тема 4. Придбання навичок з роботи з системами захисту інформації та розрахунку ризиків. Програмна система RiskWatch	8
5	Тема 5. Застосування теорії чисел в захисті інформації	8
6	Тема 6. Експертні системи виявлення зловживань (NIDES, EMERLAND, MIDAS, DIDS)м	8
7	Тема 7. Правовий статус та зміст інформації з обмеженим доступом про особу.	8
8	Тема 8 Застосування синтаксичного аналізу в виявленні вторгнень	8
9	Тема 9. Організаційно-правові основи захисту інформації з обмеженим доступом та особливості захисту певних видів інформації.	8
10	Тема 10. Захист операційних систем	8
11	Тема 11. Теоретичні та практичні аспекти побудови та застосування методів криптографічного захисту інформації в системах спеціального зв'язку, електронного документообігу та електронної комерції	10
12	Тема 12. Менеджмент інформаційної безпеки	10
13	Виконання Курсової Роботи	30
	Усього годин	130

6.5. Індивідуальні та/або групові завдання

Студенти виконують курсову роботу за темою «Розробка комплексу заходів з захисту інформації, аналіз політик інформаційної безпеки».

В процесі виконання роботи студенти проводять ідентифікацію активів обраного об'єкту, виявлення погроз інформаційної безпеки, аналіз та розрахунок ризиків; пропонують план зниження ризиків; створюють розробки з захисту інформації.

Метою роботи є аналіз ризиків та розробка комплексу заходів підвищення безпеки інформаційної системи та контроль виконання розроблених заходів.

Головна задача - здобуття навичок виділення загроз інформаційної безпеки, отримання навичок проведення внутрішнього аудиту.

7. Література

7.1. Основна

1. Белов Е.Б., Лось В.П., Мешеряков Р.В., Шелупанов А.А. Основы информационной безопасности: Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2006. – 544с
2. Варфоломеев А.А. Основы информационной безопасности: Учеб. пособие. – М.: РУДН, 2008. – 412 с
3. Галатенко В.А. Основы информационной безопасности: Курс лекций. – М.: ИНТУИТ. РУ, 2016. – 205 с
4. Голев, Д.В. Методика оцінки інформаційної захищеності телекомунікацій : Навч. посіб. галузі знань 1601, 1701 “Інформаційна безпека” за спеціальністю 7.17010201, 8.17010201 – Системи технічного захисту інформації, автоматизації її обробки. – Одеса, 2013. – 218 с.
5. Домарев В. В. Безопасность информационных технологий. – СПб.: DiaSoft, 2012. – 658 с.
6. А.В. Домашев, М.М. Грунтович, В.О. Попов, Д.И. Правиков, А.Ю. Щербаков Программирование алгоритмов защиты информации. – М.: Изд-во “Нолидж”, 2001. – 552с
7. Інформаційна безпека : навч. посіб. / Ю.Я. Бобало, І.В. Горбатий, М.Д. Кіселичник та ін. ; ред. Ю.Я. Бобало, І.В. Горбатий . – Львів : вид-во Львівської політехніки, 2019. – 580 с.
8. Конев И., Беляев А. Информационная безопасность предприятия. — СПб.: БХВ Петербург, 2003. — 752 с.
9. Лісовська, Ю.П. Інформаційна безпека України : навч. посіб. / Ю.П. Лісовська . — Київ : вид-во Кондор, 2018. — 172 с.
10. Методи безпечної обробки інформації у багатопозиційних системах радіолокації : монографія. – К. : ЦУЛ, 2019. – 230 с.
11. Методы и средства защиты информации / Под ред. Ю. С. Ковтанюка. — К.: ЮНИОР, 2003. — 501 с.
12. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства/ Шаньгин В.Ф. – М.: ДМК Пресс, 2008. – 544 с.

7.2. Допоміжна

1. Бакалінська, О. Правове забезпечення кібербезпеки в Україні / О. Бакалінська, О. Бакалінський // Підприємництво, господарство і право. 2019. № 9. — С. 100-108.
2. Баранов А. П., Зегжда Д. П., Зегжда П. Д. и др. Теоретические основы информационной безопасности: Учеб. пособие. — СПб., 1998. — 173 с.
3. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. — М.: Энергоатомиздат, 1994, Кн. 1 и 2.
4. Гайкович В., Першин А. Безопасность электронных банковских систем. — М.: Единая Европа, 1994.
5. Захаренко, К. Развитие системы информационной безопасности: опыт зарубежных стран / К. Захаренко // Вища освіта України. 2018. № 3. — С. 71-77.
6. Краснов А. В. Некоторые проблемы безопасности в сетях ЭВМ и способы их решения. Защита информации. — 1992. — № 3-4.

7. Мазаник С. Безопасность компьютера: защита от сбоев, вирусов и неисправностей / С.Мазаник. — М.: Эксмо, 2014. — 256с.
8. Медведевский И. Д., Безгачев В. А., Гореленков А. П. Информационная безопасность распределенных вычислительных систем: Руководство к практическим занятиям // Под ред. проф. П.Д.Зегжды. — СПб., 1998. — 73с.
9. Мафтик С. Механизмы защиты в сетях ЭВМ. — М.: Мир, 1993.
10. Петраков А. В., Лагутин В. С. Утечка и защита информации в телефонных каналах. — 2-е изд. — М.: Энергоатомиздат, 1997.— 304 с.
11. Расторгуев С.П. Программные методы защиты информации в компьютерах и сетях. — М.: Яхтсмен, 1993. — 188 с.
12. Шеннон К. Теория связи в секретных системах. Работы по теории информации и кибернетике. — М.: ИЛ, 1963.
13. Denning D. Cryptography and data security. Addison- Wesley Publishing Company. 1982. — 400 p.
14. Jackson K., Hruska J. (Ed.) Computer Security Reference Book. Butterworth-Heinemann Ltd., 1992. — 932 p.
15. Russel D., G.T.Gangemi Sr. Computer Security Basics. — O'Reilly & Associates, Inc., 1991. — 448 p.

7.3 Методична

1. Методичні вказівки до виконання курсових робіт з дисципліни «Інформаційна безпека» для студентів спеціальності 121 Інженерія програмного забезпечення [Електронний ресурс] / укладач Н.О. Маслова ; відповідаль. за випуск О.А. Дмитрієва . — Покровськ, 2018. — 22 с.
код НТБ ДонНТУ: М271, режим доступу
http://89.185.3.253:9080/list.php?realist=6&IDlist=Q_1&=1612813927039
2. Методичні вказівки для самостійної роботи з дисципліни «Основи інформаційної безпеки» для студентів спеціальності «Кібербезпека» денної форми навчання [Електронний ресурс] / уклад. Н.О.Маслова, О.І.Патрушева; - Покровськ: ДонНТУ, 2019. – 49с.
код НТБ ДонНТУ: М625, режим доступу
<http://ea.donntu.edu.ua/handle/123456789/30711>

8. Інформаційні ресурси

1. <http://www.alleng.ru/d/comp/comp51.htm>
2. <http://www.intuit.ru/studies/courses/10/10/info>
3. http://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0_%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0_%D0%A3%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D0%B8%D0%B4%D0%BE%D0%BA%D1%83%D0%BC%D0%B5%D0%BD%D1%82%D1%96%D0%B2_%D1%89%D0%BE%D0%B4%D0%BE_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%BE%D1%97_%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8_%D0%B2_%D0%A3%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D1%96
4. Список нормативних документів щодо інформаційної безпеки в Україні // Електр.ресурс.
http://uk.wikipedia.org/wiki/%D0%A1%D0%BF%D0%B8%D1%81%D0%BE%D0%BA_%D0%BD%D0%BE%D1%80%D0%BC%D0%B0%D1%82%D0%B8%D0%B2%D0%BD%D0%B8%D1%85_%D0%B4%D0%BE%D0%BA%D1%83%D0%BC%D0%B5%D0%BD%D1%82%D1%96%D0%B2_%D1%89%D0%BE%D0%B4%D0%BE_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%BE%D1%97_%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8_%D0%B2_%D0%A3%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D1%96